Is My Email HIPAA Compliant?

written by CPH Insurance | June 15, 2016

One of the biggest liability risks and IT myths that any medical, mental health or allied health professional can face serious liability for is the exposure from constant email correspondence and the unsecured transmission of sensitive patient information. Distinguishing between marketing fallacy and medical law reality can determine your next million-dollar lawsuit.

How can you discover the truly HIPAA Compliant email services?

HIPAA compliance requires that both data stored within the email, and data literally traveling between email systems are thoroughly encrypted throughout the process. The most important distinction is whether or not a company touts their email as being HIPAA-capable or HIPAA-compliant. HIPAA-capable is a marketing term that indicates a third party must take responsibility for any security failures within the system. A HIPAA-compliant system demands no such thing – but there is still a process to ensure that HIPAA compliant email company keeps to the standard.

When hiring a company to host your email, it's important to make sure that they sign a BAA, or Business Associate Agreement, through HIPAA. According to TechTarget.com, any business entity that serves a health care provider or institution is subject to:

1. Audits by the Office for Civil Rights (OCR) within the Department of Health and Human Services
2. Accountability for any data breach
3. Penalized for noncompliance
4. Reporting regulations for how to respond to a data breach

Is Google Apps HIPAA Compliant?

From the mouth of Google itself, they can demonstrate HIPAA compliance with Google Apps. Google is willing to set up a BAA covering the following apps:

- GMail
- Google Calendar
- Google Drive
- Google Apps Vault Services

Google has attained the security certifications such as FISMA, ISO 27001, and SSAE 16.

Is Office 365 HIPAA Compliant?

Office 365 also touts its programs as being top-notch in HIPAA compliance and patient care conscious.

Microsoft is willing to set up a BAA, but somewhat unclear as to which services it covers.

- ISO 27001 (International Organization for Standardization)
- FISMA (Federal Information Security Management Act)
- HIPAA, with Business Associate Agreement memorializing implementation of physical, technicaland administrative safeguards, and breach notification requirements of ARRA/HITECH
- EU Safe Harbor
- EU Model Clauses
- Data Processing Agreement

Microsoft has claimed that "Office 365 is more compliant than Google Apps," but I wouldn't let the rivalry get in your way of exploring both options. Just last month, the Department of Homeland Security itself warned Americans about using Microsoft's Internet Explorer. Our advice? Compare the two, research healthcare-oriented options, and most of all, never forget to make them sign that BAA! Stay covered, friends.